CLAIMS:

What is claimed is:

1. A method of encrypting data packets, comprising:

selecting a byte within a source data packet;

randomly selecting an available position within an encrypted data packet in which to place an encrypted byte corresponding to said selected byte of said source data packet;

encrypting said selected byte using a random number to generate said encrypted byte; and

placing said encrypted byte in said selected position within said encrypted data packet, wherein said selected byte of said source data packet is encrypted in an unconditionally secure manner.

2. The method of claim 1, further comprising:

repeating said steps of selecting a byte, randomly selecting an available position, encrypting said selected byte, and placing said encrypted byte in said selected position for each byte within said source data packet.

3. The method of claim 2, further comprising:

after encrypting all bytes of said source data packet, filling remaining positions within said encrypted data packet with random numbers.

4. The method of claim 2, further comprising:

after encrypting all bytes of said source data packet, encrypting authentication data; and

placing bytes of said encrypted authentication data in remaining positions within said encrypted data packet.

5. A one-time pad, comprising:

a memory device;

a nonrepeating, randomly ordered sequence of N numbers within the range of 1 to N within the memory device; and

a plurality of arrays of random numbers within said memory device, each array within said plurality of arrays associated with a number within said sequence of numbers.

6. The one-time pad of claim 5, wherein each array within the plurality of arrays comprises a character map.

7. The one-time pad of claim 5, wherein said sequence and said plurality of arrays comprise a sheet.

8. The one-time pad of claim 5, further comprising:

a counter within said memory device, said counter pointing to a sheet within a plurality of sheets within said one-time pad.

9. An electronic checkbook, comprising:

a memory containing a plurality of encryption sheets, each encryption sheet within the plurality of encryption sheets including:

a string of N numbers within the range of 1 to N arranged in a nonrepeating, randomly ordered sequence; and

a plurality of random number arrays, each array within said plurality of arrays associated with a different number within said string of numbers; and

a plurality of identifiers associating each encryption sheet within the plurality of encryption sheets with an electronic check.

10. The electronic checkbook of claim 9, wherein each encryption sheet and said associated identifier comprises an unused electronic check.

11. The electronic checkbook of claim 9, wherein said electronic check comprises information encrypted using an encryption sheet within said plurality of encryption sheets.

12. The electronic checkbook of claim 11, wherein said electronic check further comprises:

a plurality of encrypted bytes generated from a plurality of source bytes,

wherein each encrypted byte is placed in a position within said plurality of encrypted bytes identified by a position number located within said string at a location corresponding to a location within said plurality of source bytes containing a source byte utilized to generate said encrypted byte, and

wherein each encrypted byte comprises a random number corresponding, within an array associated with said position number, to said source byte.

13. The electronic checkbook of claim 12, wherein said electronic check further comprises:

authentication data encrypted with said plurality of encrypted bytes.

14. The electronic checkbook of claim 9, wherein said electronic checkbook further comprises:

~~a port for connection to a receiving device.~~

15. A method of processing an electronic check, comprising:

receiving an electronic check encrypted using a one-time pad at a business;

transmitting a first copy of said electronic check to a payor's bank and a second copy of said electronic check to a payee's bank; and

decoding said first copy of said electronic check at said payor's bank using a copy of said one-time pad.

16. The method of claim 15, further comprising:

authenticating said electronic check; and

transmitting said first copy of said electronic check to a clearinghouse with a payment authorization.

17. The method of claim 16, further comprising:

transmitting said second copy of said electronic check to said clearinghouse;

comparing said first copy of said electronic check to said second copy of said electronic check; and

responsive to determining that said first copy of said electronic check matches said second copy of said electronic check, processing a transaction transferring funds from said payor's bank to said payee's bank.

18. A method of securing transmission of a global transponder location, comprising:

receiving a request packet via a cellular communications link to said global transponder;

encrypting a data packet containing a latitude and a longitude for a location of said global transponder using a one-time pad containing within said global transponder; and

transmitting said encrypted data packet to a central computer over said cellular communications link.

19. The method of claim 18, wherein said step of encrypting a data packet further comprises:

locating an identifier within said request packet;

comparing said identifier to a plurality of identifiers in said global transponder, wherein identifier within said plurality of identifiers is associated with a sheet within said one-time pad;

responsive to determining that said identifier within said request packet does not match any identifier within said plurality of identifiers, terminating said cellular communications link; and

responsive to determining that said identifier within said request packet matches an identifier within said plurality of identifiers, encrypting said data packet using a sheet within said one-time pad associated with said matching identifier.

20. A global transponder, comprising:

a processor connected to a memory containing a one-time pad;

a cellular modem connected to said processor and an antenna;

a GPS chip set connected to said processor and said antenna, said GPS chip set providing GPS fix data to said processor,

wherein said processor, responsive to receiving a call through said cellular modem, encrypts said GPS fix data using said one-time pad for transmission via said cellular modem.

21. A method of encrypting data packets using a one-time pad, comprising:

selecting a character within a source data packet;

reading a position number within a randomly ordered, nonrepeating sequence of N numbers within the range of 1 to N, wherein said position number is at a location within said sequence corresponding to a location of said selected character within said source data packet;

reading a random number within a nonrepeating array of random numbers associated with said position number, wherein said random number corresponds within said array to said selected character; and

placing said random number in a position within an encrypted data packet corresponding to said position number.

22. The method of claim 21, further comprising:

repeating said steps of selecting a character, reading a position number, reading a random number corresponding to said selected character, and placing said random number in a position corresponding to said position number for each character within said source data packet to encrypt said source data packet.

23. The method of claim 22, further comprising:

after encrypting said source data packet, encrypting an authentication code; and

placing the encrypted authentication code within said encrypted data packet.

24. The method of claim 22, further comprising:

after encrypting said source data packet, encrypting a stop code; and

placing the encrypted stop code within said encrypted data packet.

25. A method of decoding data packets encrypted using a one-time pad, comprising:

reading a position number within a randomly ordered, nonrepeating sequence of N numbers within the range of 1 to N;

reading a random number located within an encrypted data packet at a position corresponding to said position number;

determining a character corresponding to said random number within a nonrepeating array of random numbers associated with said position number; and

placing said character in a next available position within a decoded data packet.

26. The method of claim 25, further comprising:

repeating said steps of reading a position number, reading a random number, determining a character corresponding to said random number, and placing said character in a next available position for each character in said decoded data packet.

27. The method of claim 26, further comprising:

detecting a stop code encrypted in said encrypted data packet.

28. The method of claim 26, further comprising:

decoding an authentication code encrypted in said encrypted data packet.

29. A computer program product for use with a data processing system, comprising:

a computer usable medium;

first instructions on said computer usable medium for selecting a character within a source data packet;

second instructions on said computer usable medium for reading a position number within a randomly ordered, nonrepeating sequence of N numbers within the range of 1 to N, wherein said position number is at a location within said sequence corresponding to a location of said selected character within said source data packet;

third instructions on said computer usable medium for reading a random number within a nonrepeating array of random numbers associated with said position number, wherein said random number corresponds within said array to said selected character; and

fourth instructions on said computer usable medium for placing said random number in a position within an encrypted data packet corresponding to said position number.

30. A computer program product for use with a data processing system, comprising:

a computer usable medium;

first instructions on said computer usable medium for reading a position number within a randomly ordered, nonrepeating sequence of N numbers within the range of 1 to N;

second instructions on said computer usable medium for reading a random number located within an encrypted data packet at a position corresponding to said position number;

third instructions on said computer usable medium for determining a character corresponding to said random number within a nonrepeating array of random numbers associated with said position number; and

fourth instructions on said computer usable medium for placing said character in a next available position within a decoded data packet.

Add A7